



Recover files and folders using Previous Versions

ONTAP 9

NetApp

February 12, 2026

This PDF was generated from <https://docs.netapp.com/us-en/ontap/smb-admin/recover-files-folders-previous-versions-concept.html> on February 12, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Recover files and folders using Previous Versions	1
Learn about recovering ONTAP SMB files and folders using previous versions	1
ONTAP SMB requirements for using Microsoft Previous Versions	1
ONTAP version requirements	1
SMB protocol version requirements	1
Windows client requirements	1
Requirements for snapshot settings	2
View and manage ONTAP SMB snapshot data with the Windows Previous Versions tab	2
Determine whether ONTAP SMB snapshots are available for Previous Versions use	3
Create ONTAP SMB snapshot configurations to enable Previous Versions access	4
Learn about restoring Previous Versions directories that contain ONTAP SMB junctions	5

Recover files and folders using Previous Versions

Learn about recovering ONTAP SMB files and folders using previous versions

The ability to use Microsoft Previous Versions is applicable to file systems that support snapshots in some form and have them enabled. Snapshot technology is an integral part of ONTAP. Users can recover files and folders from snapshots from their Windows client by using the Microsoft Previous Versions feature.

Previous Versions functionality provides a method for users to browse through the snapshots or to restore data from a snapshot without a storage administrator's intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made snapshots available on a share, then the user can use Previous Versions to perform the following tasks:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of file while working.

The data stored in snapshots is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshots are periodically deleted; therefore, users need to create copies of files contained in Previous Versions if they want to indefinitely retain a previous version of a file.

ONTAP SMB requirements for using Microsoft Previous Versions

Before you can use Previous Versions with your CIFS server, you need to know which versions of ONTAP and SMB, and which Windows clients, support it. You also need to know about the snapshot setting requirement.

ONTAP version requirements

Supports Previous Versions.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Previous Versions on all versions of SMB.

Windows client requirements

Before a user can use Previous Versions to access data in snapshots, the Windows client must support the feature.

For the latest information about which Windows clients support Previous Versions, see the Interoperability Matrix.

Requirements for snapshot settings

To use Previous Versions to access data in snapshots, an enabled snapshot policy must be associated to the volume containing the data, clients must be able to access to the snapshot data, and snapshots must exist.

View and manage ONTAP SMB snapshot data with the Windows Previous Versions tab

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in snapshots without needing to involve the storage virtual machine (SVM) administrator.

About this task

You can only use the Previous Versions tab to view and manage data in snapshots of data stored on the SVM if the administrator has enabled snapshots on the volume containing the share, and if the administrator configures the share to show snapshots.

Steps

1. In Windows Explorer, display the contents of the mapped drive of the data stored on the CIFS server.
2. Right-click the file or folder in the mapped network drive whose snapshots you want to view or manage.
3. Click **Properties**.

Properties for the file or folder you selected are displayed.

4. Click the **Previous Versions** tab.

A list of available snapshots of the selected file or folder is displayed in the Folder versions: box. The listed snapshots are identified by the snapshot name prefix and the creation timestamp.

5. In the **Folder versions:** box, right-click the copy of the file or folder that you want to manage.
6. Perform the appropriate action:

If you want to...	Do the following...
View data from that snapshot	Click Open .
Create a copy of data from that snapshot	Click Copy .

Data in snapshots is read-only. If you want to make modifications to files and folders listed in the Previous Versions tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

7. After you finish managing snapshot data, close the **Properties** dialog box by clicking **OK**.

For more information about using the Previous Versions tab to view and manage snapshot data, consult the Microsoft TechNet Library.

Related information

Determine whether ONTAP SMB snapshots are available for Previous Versions use

You can view snapshots from the Previous Versions tab only if an enabled snapshot policy is applied to the volume containing the share, and if the volume configuration allows access to snapshots. Determining snapshot availability is helpful when assisting a user with Previous Versions access.

Steps

1. Determine whether the volume on which the share data resides has automatic snapshots enabled and whether clients have access to snapshot directories: `volume show -vserver vserver-name -volume volume-name -fields vserver, volume, snapdir-access, snapshot-policy, snapshot-count`

The output displays what snapshot policy is associated with the volume, whether client snapshot directory access is enabled, and the number of available snapshots.

2. Determine whether the associated snapshot policy is enabled: `volume snapshot policy show -policy policy-name`
3. List the available snapshots: `volume snapshot show -volume volume_name`

For more information about configuring and managing snapshot policies and snapshot schedules, see [Data Protection](#).

Example

The following example displays information about snapshot policies associated with the volume named "data1" that contains the shared data and available snapshots on "data1".

```

cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true           default        10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
          Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true      Default policy with hourly, daily &
weekly schedules.
      Schedule      Count      Prefix          SnapMirror Label
-----
      hourly        6          hourly          -
      daily         2          daily           daily
      weekly        2          weekly          weekly

cluster1::> volume snapshot show -volume data1
                                         ---Blocks---
Vserver  Volume  Snapshot          State      Size Total% Used%
-----
vs1      data1
          weekly.2012-12-16_0015  valid    408KB  0%  1%
          daily.2012-12-22_0010  valid    420KB  0%  1%
          daily.2012-12-23_0010  valid    192KB  0%  0%
          weekly.2012-12-23_0015  valid    360KB  0%  1%
          hourly.2012-12-23_1405  valid    196KB  0%  0%
          hourly.2012-12-23_1505  valid    196KB  0%  0%
          hourly.2012-12-23_1605  valid    212KB  0%  0%
          hourly.2012-12-23_1705  valid    136KB  0%  0%
          hourly.2012-12-23_1805  valid    200KB  0%  0%
          hourly.2012-12-23_1905  valid    184KB  0%  0%

```

Related information

- [Create snapshot configurations to enable Previous Versions access](#)
- [Data protection](#)

Create ONTAP SMB snapshot configurations to enable Previous Versions access

The Previous Versions functionality is always available, provided that client access to snapshots is enabled and provided that snapshots exist. If your snapshot configuration

does not meet these requirements, you can create a snapshot configuration that does.

Steps

1. If the volume containing the share to which you want to allow Previous Versions access does not have an associated snapshot policy, associate a snapshot policy to the volume and enable it by using the `volume modify` command.

Learn more about `volume modify` in the [ONTAP command reference](#).

2. Enable access to the snapshots by using the `volume modify` command to set the `-snap-dir` option to `true`.

Learn more about `volume modify` in the [ONTAP command reference](#).

3. Verify that snapshot policies are enabled and that access to snapshot directories is enabled by using the `volume show` and `volume snapshot policy show` commands.

Learn more about `volume show` and `volume snapshot policy show` in the [ONTAP command reference](#).

For more information about configuring and managing snapshot policies and snapshot schedules, see [Data Protection](#).

Related information

[Data protection](#)

Learn about restoring Previous Versions directories that contain ONTAP SMB junctions

There are certain guidelines you should keep in mind when using Previous Versions to restore folders that contain junction points.

When using Previous Versions to restore folders that have child folders that are junction points, the restore can fail with an `Access Denied` error.

You can determine whether the folder that you are attempting to restore contains a junction by using the `vol show` command with the `-parent` option. You can also use the `vserver security trace` commands to create detailed logs about file and folder access issues.

Related information

[Creating and managing data volumes in NAS namespaces](#)

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—with prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.